RADFORD UNIVERSITY

Policy Title: Facilities Access Control Policy	**Effective Date: 4/1/2019**
Policy Number: FA-PO-1210	**Date of Last Review: NEW**
Oversight Department: Facilities Management and University Services	**Next Review Date: 4/1/2022**

1. PURPOSE

The *Facilities Access Control Policy* for Radford University (University) is intended to facilitate, and appropriately limit, access to University facilities by authorized users in order to ensure the safety and protection of the University community and property. The policy outlines the responsibilities for maintaining a secure environment and establishes the process for granting/removing access privileges, issuing keys and access cards, and periodically reviewing access privileges.

2. APPLICABILITY

The *Facilities Access Control Policy* applies to all University students, employees, contractors, and authorized visitors or organizations.

3. DEFINITIONS

Access Card: A University identification (ID) or similar card issued by the RU Express/ID Card Office for the purpose of accessing University facilities. An access card may be magnetic stripe, proximity, biometric, or chip enabled.

Access Reader: An approved device equipped to read the media of an access card to approve or deny entry to a specific University facility. These devices are connected to the IP-based door access system via the University's information technology network.

Authorized Visitor: For the purposes of this policy, any person other than a student, employee, or contractor requiring access via key or access card to secured University facilities in order to perform their function. Such persons must follow this policy for obtaining access.

CT (Control) Key: Keys that grant access to University facilities requiring the highest level of security. Master Keys cannot be used to access these secure areas. Examples include the Police evidence room, Police armory, and Student Health Center pharmaceuticals storage room.

Division Head: The President, Provost, or applicable Vice President.

Electronic Access: Equipment and related processes and procedures designed to use University-issued credentials as a means to control access to specific University facilities. Electronic access replaces traditional keys with access readers to read access cards and thereby allow or deny entry to a University facility.

Electronic Access Approver: Persons within a unit who are responsible for granting or removing access, within the University's door access system, to University facilities to which they have been given authority to oversee.

Electronic Access Controls: Access readers and other related equipment that read the media on University issued credentials to restrict or allow access to facilities.

Electronic Door Access System: The University's ID card system that provides, among other system capabilities, the technology behind the IP-based door access control.

Key: Refers to a traditional, physical key used with a lockset to maintain access to University facilities. These physical devices fall under the oversight of Facilities Management.

Key Custodian: A designated employee responsible for the distribution, monitoring, and collection of keys for specific University facilities.

Key Exchange Box: A device used to securely store a key, which can only be accessed via the use of a key that becomes trapped in the device until the secured key is returned to the device.

Master Key: Keys that grant access to multiple buildings, an entire building, or substantial parts of a building.

Standard Operational Key: Keys that grant access to areas such as offices, file/storage rooms, conference rooms, classrooms, etc.

Sub-Master Key: Keys that grant access to areas within a building such as a suite or group of departmental offices.

University Community: For the purposes of this policy, all persons who are University students, employees, contractors, and authorized visitors or organizations.

University Facility/Facilities: For the purpose of this policy, University facilities include all property, buildings, and rooms owned, leased, or controlled by the University.

4. POLICY

A. The security of University facilities will be a priority for all members of the University community.

B. The University will use one of several means to grant, restrict, or modify a person's access to University facilities in order to secure persons and property. The University will, by default, install a means of securing facilities using keys. In areas where there is a need to more closely monitor and control access to facilities, the University may choose to add electronic access controls.

C. Facilities Management will have sole authority and responsibility for installing all locksets and making/issuing related keys to access University facilities. Facilities Management is also responsible for changing combinations on all mechanical keypads. Additionally, Facilities Management will have sole responsibility for installing and maintaining all card access door hardware, including but not limited to, electric strikes, door position contacts, local alarms, and all related wiring.

D. University Services will have sole authority and responsibility for issuing access cards, providing electronic card access to University facilities, and administering the University's door access system. University Services will coordinate with Division of Information

Technology and Facilities Maintenance and Operations on all electronic access installations and maintenance.

E. All vendors contracted by the University to provide private security services under the auspices of this policy must be licensed by the Virginia Department of Criminal Justice Services in accordance with Code of Virginia § 9.1-138 et seq.

F. Unauthorized locks are prohibited on all doors and, if found, will be removed and discarded. Any damage or repair necessitated by the removal of unauthorized locks will be the responsibility of the department or person found in violation of this policy.

G. All keys issued for an indefinite period of time must be assigned to a person with a University ID number. Exceptions must be approved by the appropriate Division Head.

H. Access privileges will be assigned based upon a person's role, residential or class assignment, and/or job responsibilities. Access privileges may be removed and/or suspended upon approval of the University Administration or University Police.

I. An employee's immediate supervisor is responsible for ensuring that all keys/access cards are returned as required when an employee no longer needs the particular access, whether due to a separation, transfer within the University, or change in job responsibilities.

J. Each person assigned a key/access card is responsible for protecting the security of the key/access card. All keys/access cards will remain the property of the University. Keys/access cards must never be shared. Lost keys/access cards must be reported immediately to an employee's supervisor, or the appropriate Residential Life Staff member, and the Radford University Police Department in accordance with this policy.

K. Unauthorized duplication of University issued keys/access cards is strictly prohibited. Any persons found to have duplicated, or attempted to duplicate, keys/access cards may be subject to disciplinary and/or legal action as may be appropriate in the circumstances.

L. No person may knowingly possess University keys/access cards without proper authorization. Additionally, no person may attempt to gain unauthorized access to any University facilities.

M. The University regards any violation of this policy as a serious threat to security, including security compromises facilitated by failure to remove access or retrieve keys from departing users when access to University facilities is no longer required. Violators of this policy may be subject to disciplinary action and may also be subject to prosecution under relevant federal, state, or local laws.

5. PROCEDURES

A. <u>Key Control</u>

1. Key Security and Control:

a. All equipment used to cut keys will be located in Facilities Management in a secure and alarmed room used for the purpose of key control.

b. All keys issued to employees on a permanent basis must be retained in the possession or control of the authorized employee. An employee is authorized to use the issued keys for the sole purpose of carrying out his or her job responsibilities.

c. Keys are limited to one key per facility or area per person unless otherwise approved.

d. Keys that are no longer needed, or have become obsolete, must be returned to Facilities Management for appropriate retention or disposal.

e. Master Keys should not leave University owned, leased, or controlled property and must be stored on such property in a key exchange box approved by Facilities Management.

f. Facilities Management will develop and implement an appropriate schedule to review keys issued to ensure appropriate security and control is maintained.

g. Deans, Associate/Assistant Vice Presidents, or Directors may designate an employee as Key Custodian for a particular department or office by completing and signing the *Key Control Form* (see Appendix A) and sending it to Facilities Management. *Procedures for Key Custodians* are included in Appendix B.

h. Facilities Management will maintain an inventory of keys to be issued to contractors for a defined period of time while performing work on University facilities. These keys will be issued directly to a University employee who will be responsible for ensuring the keys are returned by the contractor at the appropriate time.

2. Key Issuance/Return/Transfer:

a. All requests for keys must be submitted to Facilities Management (Box 6909 or Fax 831-7783) on an approved *Key/Lock Request Form* (see Appendix A). The form must include the following information:

i. Name of supervisor submitting the request

ii. Date of request

iii. Building

iv. Department

v. Phone number of supervisor

vi. Banner organization code

vii. Key number (if known)

viii. Quantity

ix. Door or room number

x. Name of person to whom key will be assigned

xi. Radford University Identification (RU ID) Number

xii. Email address of the person to whom key will be assigned

xiii. Nature/description of request

xiv. Authorizing Signature(s) as follows:

(a) Standard Operational Key – Dean, Associate/Assistant Vice President, Director, Department Chair, or other supervisor organizationally responsible for the applicable facility (see Building Steward List, Appendix D, of the *Use of University Facilities Policy*).

(b) Sub-Master Key – Dean, Associate/Assistant Vice President, or Director

(c) Master Key – Chief of Police and Division Head

(d) CT (Control Key) – Chief of Police and Division Head

(e) Keys issued to non-employees – Division Head

b. Keys returned to Facilities Management must be accompanied by a completed *Returned Keys Form* (see Appendix A).

c. When the possession or control of a key or keys changes from on person to another, a *Key Transfer Form* (see Appendix A), with appropriate approvals, must be submitted to Facilities Management.

3. Lost Keys:

a. Any person assigned a University key must report lost keys immediately to their immediate supervisor or, in the case of University residents, to an appropriate Residential Life Staff member. The Radford University Police Department must also be notified immediately of any lost key.

b. The Radford University Police Department and immediate supervisor must notify Facilities Maintenance and Operations upon notification of a lost key.

c. Departments may be responsible for any costs incurred to secure an area when a key is lost.

4. Access/Lock Issues:

a. Any issues with key access (e.g. an area cannot be accessed or secured) should be reported to Facilities Management at 831-7800 or facilities@radford.edu during normal business hours (7:30 am to 5:00 pm, Monday through Friday). After normal business hours and on weekends, issues with key access must be reported to the Radford University Police Department at 831-5500.

b. All requests to install or remove any type of locking mechanism on any door must be submitted to Facilities Management on an approved *Facilities Management Service Request Form (PP25)* (see Appendix C). Departments may be responsible for any costs associated with the service request.

B. Electronic Access Controls

1. Electronic Access Security and Control

a. Granting and removing electronic access privileges to University facilities for all persons or groups of persons will be completed using the Electronic Door Access System, which is under the oversight of the Director of University Services. The Auxiliary Services Technician Team Lead in IT Infrastructure (System Administrator) assists with many administrative responsibilities related to the Electronic Door Access System.

b. As the University has designated the Electronic Door Access System as a sensitive system, any user with any level of access to the Electronic Door Access System must complete the *CS Gold System Access Request* (contact the Director of University Services to obtain the form) and submit the form to the Director of University Services for approval.

c. Persons will be granted access within the Electronic Door Access System on a least privilege basis as supported by documented business need. Access to the Electronic Door Access System is accomplished by assigning each person to an appropriate access group within the system. University Services will develop and implement an appropriate schedule to review access to ensure appropriate security and control is maintained.

d. The Emergency Lock Down feature in the Electronic Door Access System is intended for use by the University Police Department. When this feature is enabled, all electronic card access, except for University Police Officers and select University Services staff, will be suspended in order to control access to University facilities in the event of situations deemed as warranting such action. The Chief of Police will have the authority to determine the parameters that will dictate the use of this feature.

2. Granting and Removing Facility Electronic Access Privileges

a. Electronic access to residence halls will be granted to students that are assigned to a specific residence hall for the period of time indicated by Residential Life, which is typically one academic term. Such access will be granted via an automatic download from the Housing System to the Electronic Door Access System and will be identified in the student's Electronic Door Access System account as having been granted by Residential Life. Staff from Residential Life with access to the Electronic Door Access System (see Section 5.B.1.b) are also permitted to add and remove a residence hall occupant's access to one or more residence halls as needed. At the end of each academic term, student electronic access to residence halls will also be automatically suspended and/or removed by the System Administrator.

b. Electronic access to specific academic and administrative facilities will be granted by the System Administrator as follows:

i. Certain academic facilities with electronic access are associated with classes in Banner and, once students are enrolled in those classes, the students will be given electronic access to the facilities for the related academic term.

ii. Faculty teaching classes in academic facilities with electronic access may also provide a list of classes to the System Administrator to have students enrolled in those classes provided electronic access to the facilities for the related academic term.

iii. University employees and students will be provided access to certain other University facilities based on their classification and active status in accordance with internal procedures.

c. Electronic access to specific spaces within residence halls and academic/administrative facilities may also be requested by completing a *Door Access Request* (see Appendix D). Requests for access to residence halls must be approved by the Office of Residential Life. Requests for access to academic/administrative facilities must be approved by a Dean, Associate/Assistant Vice President, Director, Department Chair, or other supervisor organizationally responsible for the applicable facility (see Building Steward List, Appendix D, of the *Use of University Facilities Policy*).

d. At the end of each academic term, electronic access provided to students for academic and administrative facilities will be removed by the System Administrator. Access for subsequent academic terms must be reassigned using the same process as described above. Requests for exceptions to allow a student to maintain electronic access to specific University facilities during breaks, or beyond the end of the academic term, must be communicated in writing to the Director of University Services or the System Administrator, and must include the specific period for which the access applies. The termination date for such electronic access will be manually monitored and removed by the System Administrator as appropriate.

e. As applicable, Deans, Associate/Assistant Vice Presidents, or Directors may designate an Electronic Access Approver (see Section 5.B.1.b.). The Electronic Access Approver will be able to add or remove electronic access for applicable academic and administrative facilities on a case by case basis without prior approval from the Director of University Services.

f. Employee electronic access will be removed as a part of the employee separation process as defined by the Department of Human Resources. The employee separation process is initiated by the employee's supervisor. As a part of the separation process, emails will be sent notifying University Services of the separation. Once the email is received, University Services removes the access as appropriate.

g. In situations where access is no longer needed other than terminations (e.g. employees transferring between departments, changes in employee duties, etc.) the supervisor must contact the Director of University Services or System Administrator directly and request removal of the access.

h. For students who withdraw from the University through the withdrawal process, the Office of the Registrar will notify University Services via email. Once the email is received, University Services will remove the access as appropriate.

3. Requests for Electronic Access Installation:

a. Existing Facilities –

i. Any area requesting electronic access to be installed must first submit a *Facilities Management Service Request Form (PP25)* (see Appendix C) to Facilities Management. The PP25 must be approved by the applicable Division Head or Dean and a written justification of the business need for the electronic access requested must accompany the form.

ii. Facilities Management will review the PP25 and confirm whether the addition of the electronic access will meet all applicable regulatory requirements. If the review confirms that all applicable regulatory requirements can be met, Facilities Management will then forward the PP25 to the Radford University Police Department for review and comment. Facilities Management will also issue any permits that may be needed in order for the installation to be completed.

iii. The Radford University Police Department will review the PP25 for any safety and security concerns. If the Radford University Police Department finds that there is sufficient justification for the installation of the electronic access, the Chief of Police will forward a written recommendation to the Director of University Services.

iv. Once the written recommendation from the Radford University Police Chief is received, the Director of University Services will initiate a review of the request in order to provide an estimate of costs for the installation. The estimate will include all one-time and reoccurring costs associated with the installation.

v. Once the estimate is completed, the Director of University Services will share the estimate with the requestor. If the requestor approves of the estimated costs, the requestor must provide the appropriate budget information to the Director of University Services in order for the equipment to be ordered and the project to begin.

vi. University Services will place all orders for the project and coordinate the project schedule. University Services will also coordinate with the requestor for bringing the location(s) of electronic access online to include, but not limited to, scheduling door lock/unlock schedules.

b. Capital Construction and Major Renovations –

i. All new University facilities will have electronic access installed on all exterior, public use doors along with a backup Master Key set as designated by Facilities Management. All interior doors will be installed with traditional keys and locksets as determined by Facilities Management.

ii. The electronic locking/unlocking schedule for the new facility will be determined by the appropriate Division Head and the Vice President for Finance and Administration & Chief Financial Officer.

iii. Any request for electronic access to interior doors should be made and evaluated during the planning phase for construction. The written request for interior electronic access must be submitted to the Director of Facilities Planning and Construction. Final approval for interior electronic access will be obtained by the Director of Facilities Planning and Construction from the applicable Division Head in consultation with the Vice President for Finance and Administration & Chief Financial Officer. Areas that may fall into this category include, but are not limited to, areas where sensitive data is housed, areas where hazardous materials are stored, areas housing property of significant value, or areas where it is mandated by an external authority in order to maintain operational or credentialed status.

6. EXCLUSIONS

None.

7. APPENDICES

Appendix A: Facilities Management Key Forms

Appendix B: Procedures for Key Custodians

Appendix C: Facilities Management Service Request Form (PP25)

Appendix D: Door Access Request (coming soon)

8. REFERENCES

Code of Virginia, § 9.1-138 et seq., "Private Security Services Businesses."

9. INTERPRETATION

The authority to interpret this policy rests with the President of the University and is generally delegated to the Vice President for Finance and Administration & Chief Financial Officer.

10. APPROVAL AND REVISIONS

The *Facilities Access Control Policy* replaces and expands upon the Key Control and Lock Policy developed by Facilities Management. The new *Facilities Access Control Policy* was submitted to and approved by the President's Cabinet at the meeting on February 4, 2019. President Hemphill signed the policy on February 4, 2019.

For general information concerning University policies, contact the Office of Policy Compliance – (540) 831-5794. For questions or guidance on a specific policy, contact the Oversight Department referenced in the policy.